

Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1-31. (Cancelled)

32. (Previously Presented) A computer-implemented method for managing access to encrypted electronic documents, comprising:

providing in an access controlled manner multiple skeleton decryption keys for multiple encrypted documents, where a single skeleton key can be used to open multiple encrypted documents, a single encrypted document can be opened using more than one skeleton key, and a single skeleton key can be opened using one or more other skeleton keys;

each single skeleton key being a key usable to decrypt one or more secondary decryption keys; and

each secondary decryption key being a skeleton key or a decryption key for an encrypted document;

whereby one or more skeleton keys can be issued for a document or a set of documents, and a holder of a particular skeleton key can open any document to which the particular skeleton key applies, directly or indirectly.

33. (Original) The method of claim 32, wherein the skeleton keys are distributed to users in rights management files.

34-35. (Cancelled)

36. (Previously Presented) A computer program product, tangibly embodied on a machine-readable medium, for managing access to encrypted electronic documents, comprising

instructions operable to cause a programmable processor to:

provide in an access controlled manner multiple skeleton decryption keys for multiple encrypted documents, where a single skeleton key can be used to open multiple encrypted documents, a single encrypted document can be opened using more than one skeleton key, and a single skeleton key can be opened using one or more other skeleton keys;

each single skeleton key being a key usable to decrypt one or more secondary decryption keys; and

each secondary decryption key being a skeleton key or a decryption key for an encrypted document;

whereby one or more skeleton keys can be issued for a document or a set of documents, and a holder of a particular skeleton key can open any document to which the particular skeleton key applies, directly or indirectly.

37-38. (Canceled)

39. (New) The method of claim 33, wherein the rights management files are specific to particular users.

40. (New) The method of claim 33, wherein the rights management files are specific to a particular user-operated system.

41. (New) The method of claim 32, further comprising encrypting documents and skeleton keys in a symmetric manner.

42. (New) The method of claim 32, further comprising encrypting documents and skeleton keys in an asymmetric manner.

43. (New) The product of claim 36, wherein the skeleton keys are distributed to users in rights management files.

44. (New) The product of claim 43, wherein the rights management files are specific to particular users.

45. (New) The product of claim 43, wherein the rights management files are specific to a particular user-operated system.

46. (New) The product of claim 36, further comprising encrypting documents and skeleton keys in a symmetric manner.

47. (New) The product of claim 36, further comprising encrypting documents and skeleton keys in an asymmetric manner.

48. (New) A system comprising:
means for providing in an access controlled manner multiple skeleton decryption keys for multiple encrypted documents, where a single skeleton key can be used to open multiple encrypted documents, a single encrypted document can be opened using more than one skeleton key, and a single skeleton key can be opened using one or more other skeleton keys;
each single skeleton key being a key usable to decrypt one or more secondary decryption keys; and
each secondary decryption key being a skeleton key or a decryption key for an encrypted document;
whereby one or more skeleton keys can be issued for a document or a set of documents, and a holder of a particular skeleton key can open any document to which the particular skeleton key applies, directly or indirectly.

49. (New) The system of claim 48, wherein the skeleton keys are distributed to users in rights management files.

50. (New) The system of claim 49, wherein the rights management files are specific to particular users.

51. (New) The system of claim 49, wherein the rights management files are specific to a particular user-operated system.

52. (New) The system of claim 48, further comprising encrypting documents and skeleton keys in a symmetric manner.

53. (New) The system of claim 48, further comprising encrypting documents and skeleton keys in an asymmetric manner.